UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

TREVOR SLOAN, JOSEPH BLEIBERG, ARYEH LOUIS ROTHBERGER, PATRICK COMMERFORD, KEVIN FARR, ELMER ORPILLA, KEITH LAPATING, and SAGAR DESAI, on behalf of themselves and all others similarly situated, Plaintiffs, v. ANKER INNOVATIONS LIMITED, FANTASIA TRADING LLC, and POWER MOBILE LIFE LLC, Defendants.	Case No.: 1:22-cv-07174 Honorable Sara L. Ellis

PLAINTIFFS' MEMORANDUM OF LAW IN OPPOSITION TO DEFENDANTS' MOTION TO DISMISS CONSOLIDATED CLASS ACTION COMPLAINT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Rules

I. INTRODUCTION

Plaintiffs are purchasers of Defendants Anker Innovations Limited ("Anker Innovations"), Fantasia Trading LLC ("Fantasia") and Power Mobile Life LLC's ("Power Mobile," and, together with Anker Innovations and Fantasia, "Defendants") "eufy" branded home video security cameras (the "Camera Products").[1] Defendants touted that their Camera Products, which could differentiate between residents and visitors using facial-recognition technology, saved all video recordings and conducted all facial recognition *locally* (meaning on equipment located with and controlled by consumers). Indeed, Defendants emphasized that Anker Camera Products were different from competitors' products because (i) "your recorded footage will be kept private. ***Stored locally***. ***With military-grade encryption***. ***And transmitted to you, and only you***," (ii) "we're taking every step imaginable to ***ensure that your data remains private, with you***," (iii) "***[Y]our private data never leaves the safety of your home, and is accessible by you alone***," and (iv) "***There is no online link available to any video***." Although Defendants repeated the above privacy and security promises to consumers on the Camera Products' packaging, Anker's website, Amazon.com, and Google and Apple "app stores"—in the hopes that consumers would choose Anker's Camera Products over products from competitors like Google—***none of these statements were true***. In fact, later after initially denying their falsity, Defendants ultimately admitted these representations were untrue.

Plaintiffs and other consumers reviewed Anker's false and misleading marketing statements, reasonably relied on them when purchasing the Camera Products, and did not receive the products that they were promised. Moreover, Defendants uploaded Plaintiffs' and other individuals' biometric information to third-party servers without authorization. Accordingly, Plaintiffs bring this class action to recover restitution and damages, and for injunctive relief on

[1] "Camera Products" collectively refers to eufycam, Video Smart Lock, SoloCam, Floodlight Cam, Video Doorbell, and Solo Indoorcam lines of home security cameras. ¶ 1.

behalf of a nationwide class and/or classes of consumers in Illinois, New York, Massachusetts, and Florida. Plaintiffs allege that Defendants violated the Illinois Consumer Fraud and Deceptive Trade Practices Act ("ICFA"), 815 ILCS 505/1, the New York Deceptive Acts and Practices Law, Gen. Bus. ("NY GBL"), §§ 349 & 350, the Federal Wiretap Act ("Wiretap Act"), 8 U.S.C. § 2510, the Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1, the Massachusetts Consumer Protection Law ("MCPL"), Mass. G. L. 93A, and the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), Fla. Stat. § 501.201, and were unjustly enriched.

Since Defendants have ***admitted*** that: (1) they made inaccurate statements about the Camera Products' privacy and security features, and (2) and uploaded biometric data to third parties without authorization, they cannot seriously dispute that, as alleged in Plaintiffs' Complaint,[2] they violated the above privacy and consumer protection statutes and were unjustly enriched. Nevertheless, Defendants' Motion to Dismiss the Complaint[3] raises a variety of pedantic quibbles with the Complaint's language, including that (i) Anker could not have violated the Wiretap Act because it was a "party" to communications meant solely for Plaintiffs and did not "intercept" those communications within the meaning of the Act, (ii) biological identifying information is ostensibly not "biometric data" under BIPA, (iii) Defendants' admittedly false statements to consumers are not deceptive acts or practices under ICFA, NY GBL, FDUTPA and MCPL, and (iv) alleging wrongful acts by ***all*** Defendants is improper under Rule 8 of the Federal Rules of Civil Procedure, despite iron-clad black letter law to the contrary. As set forth below, these and other contentions are meritless, and the Court should deny Defendants' Motion.

[2] References to the "Complaint" are to Plaintiffs' Consolidated Class Action Complaint. ECF No. 31. Citations to "¶ __" or "¶¶ __" are to paragraphs of the Complaint. Capitalized terms not defined herein shall have the meanings set forth in the Complaint. For ease of reading, all emphasis is added and all internal quotations and citations in case citations are omitted unless otherwise indicated.

[3] References to the "Motion" or "Mot." are to Defendants' Memorandum in Support of Motion to Dismiss Consolidated Class Action Complaint. ECF No. 45-1.

II. FACTUAL BACKGROUND

Anker markets, distributes, and sells its "eufy" branded security products, including the Camera Products, throughout the United States. ¶ 27. Consumers can purchase Camera Products online directly through Anker or another online retailer or at brick-and-mortar stores. *Id.* The Camera Products allow consumers to view live and recorded video of within and around their homes and automatically receive notifications via the eufy Security smartphone application (the "eufy App"), which users must install by providing email addresses and other personally identifiable information. ¶¶ 27, 29. The Camera Products can differentiate between known individuals and strangers by comparing details about face geometry against data stored in a database. ¶ 28.

A. Defendants Misrepresent the Products' Privacy and Security Features

Facial recognition presents substantial consumer privacy concerns since, among other things, an individual's face can be used to open an app, program or cellular phone, and, unlike a password, a face template *cannot* be changed. ¶ 39. Knowing that privacy and security were essential to consumers, Anker designed and conducted a long-term marketing campaign touting the supposed privacy and security features of the Camera Products. ¶ 31.

For example, each Camera Product label stated that "Your Privacy is something that we value as much as you do," "we're taking every step imaginable to ensure that your data remains private, with you," "[w]hether it's your newborn crying for mom, or your victory dance after a game, your recorded footage will be kept private," data is "[s]tored locally" "[w]ith military-grade encryption," and "transmitted to you, and only you." ¶ 32. The label further warranted that "[a]ll your footage is securely stored locally[,] [e]nsuring the videos you record are for you and only you" and the Products have "Military-Grade AES-256 data encryption." *Id.* Anker's website repeated substantively identical promises to consumers in a "Privacy Commitment," which further warranted that "[t]here is no online link available to any video." ¶ 33. The website also included a "privacy

policy" that did not disclose that Camera Products collected or stored video and facial recognition information. ¶ 34. In addition, in the Google Play and Apple App stores Defendants represented that "[n]o data [is] shared with third parties." ¶ 36. Consumers purchased the Camera Products in reliance on these and other statements about Anker's privacy and security features and either would have paid less or not purchased the products at all but for those representations. ¶ 38.

These representations, however, were false. On November 23, 2022, security researcher Paul Moore posted a string of tweets and videos, demonstrating that the Camera Products were uploading name-tagged thumbnail images, *i.e.*, biometric information, to Anker's Amazon Web Services ("AWS") hosted cloud storage without encryption, and that the products' existing encryption was very weak and not "Military-Grade AES-256." ¶¶ 42-43. One day later, a security firm disclosed that it had found a similar transfer of thumbnails and the presence of weak encryption keys. ¶ 44. Technology media outlet *The Verge* reported that it "repeatedly watched live footage from two of our own eufy cameras . . . proving that Anker has a way to bypass encryption and access these supposedly secure cameras through the cloud." ¶ 45.

B. Defendants Are Forced to Admit That the Camera Products Transmitted Images and Biometric Information to Cloud Storage

Defendants eventually admitted that they were aware that their cameras transmitted images and biometric information to their AWS-hosted cloud storage. ¶ 55. In an email to *The Verge*, a eufy "Customer Service Engineer specialized in safety and privacy" wrote that "the app needs to communicate with the cloud server *in real-time*," *i.e.*, transmit images to cloud storage and use cloud-based facial recognition technology to compare images, and claimed to be developing a new product that would function differently. *Id.* Defendants issued a statement on November 29, 2022 conceding that thumbnails of videos are transmitted to and hosted on a cloud server maintained by a third party, namely AWS. ¶ 56. Defendants also said they were "revising the push notifications

language in the eufy App to clearly detail that push notification with thumbnails require preview images that will be temporarily stored in the cloud," and that they "will be more clear about the use of cloud for push notifications in our consumer-facing marketing materials." *Id.*

On January 31, 2023, *The Verge* revealed that "Anker has finally admitted its eufy security cameras are not natively end-to-end encrypted—they can and did produce unencrypted video streams for eufy's web portal, like the ones we accessed from across the United States using an ordinary media player." ¶¶ 64-65. While Defendants assured *The Verge* that the Camera Products finally had end-to-end encryption for "all videos (live and recorded) shared between the user's device to the eufy Security Web portal or the eufy Security App," the damage was done. *See* ¶ 65.

III. STANDARD ON MOTION TO DISMISS

On a motion to dismiss, the Court "accept[s] all well-pleaded facts as true and draw[s] all reasonable inferences in the plaintiff's favor. *White v. United Airlines, Inc.*, 987 F.3d 616, 620 (7th Cir. 2021). In considering a motion to dismiss, courts merely test the sufficiency of the allegations. *Hughes v. Huron Consulting Grp., Inc.*, 733 F. Supp. 2d 943, 946 (N.D. Ill. 2010). A motion to dismiss may not be used to dispute the well-pleaded allegations of the complaint, assess credibility, or evaluate evidence. *See, e.g.*, *City of Sterling Heights Gen. Emps. Ret. Sys. v. Hospira, Inc.*, 2013 WL 566805, at *37-38 (N.D. Ill. Feb. 13, 2013).

IV. ARGUMENT

A. Plaintiffs Have Alleged a Valid Wiretap Act Claim

The Wiretap Act prohibits "intentionally intercept[ing], endeavor[ing] to intercept, or procur[ing] any other person to intercept or endeavor to intercept, any wire, oral, or electronic communications[.]" 18 U.S.C. § 2511(1)(a). The Seventh Circuit has not decided whether a contemporaneous interception is required for wiretap claims involving electronic communications. It has, however, sustained claims regarding communications that met the "contemporaneous"

standard. *Epstein v. Epstein*, 843 F.3d 1147, 1149-51 (7th Cir. 2016). Parties to a communication or parties who received prior consent are exempt from 2511(1)(a). 18 U.S.C. § 2511(2)(d).

1. Defendants' Interception Was "Contemporaneous"

Although the Seventh Circuit has not adopted the "contemporaneous" requirement, even if the requirement applied, Plaintiffs sufficiently allege that Defendants' interceptions were contemporaneous with Plaintiffs' communications. Camera Products produce notifications when alerting consumers, including Plaintiffs, of activity. Plaintiffs understood that notifications were produced when Camera Products "captured movement[,]" or put differently, while in the midst of recording "activity detected by the cameras, including thumbnail images when a person is detected in the cameras' field of view or when a person presses the doorbell." ¶ 27, *see also* ¶¶ 14-18. Rather than apply a strict definition of "contemporaneous," the Seventh Circuit held that the contemporaneous component of the Wiretap Act is satisfied where an interception occurs "within a second" after the communication's arrival. *U.S. v. Szymuszkiewicz*, 622 F.3d 701, 705-06 (7th Cir. 2010) (rejecting that "contemporaneous" in the Wiretap Act required that a communication be "in flight"). This is true where interception occurs at a routing point for the destination rather than the destination. *See id.* ("[the computer] was effectively acting as just another router . . . [and] the Wiretap Act applies to messages that reside briefly in the memory of . . . routers").

In this case, the interception occurred not only when Defendants received the thumbnail and biometric information, but also when the data was copied. *See Epstein*, 843 F.3d at 1150 (reversing district court's dismissal of wiretap act claims where the "judge misunderstood when an interception occurs"). For the biometric data, Defendants admit that owner information, including facial identification information, was tied to some snapshots and shared with Defendants' Amazon-hosted servers before finishing the transmission of that data to other Camera Products on users' wi-fi. ¶¶ 55-59.

This case is distinct from those cited by Defendants. *See* Mot. at 10-11 (citing *In re Vizio, Inc.*, 238 F. Supp. 3d 1204, 1228 (C.D. Cal. March 2, 2017); *Rosenow v. Facebook, Inc.*, 2020 WL 1984062 at *7 (S.D. Cal. April 27, 2020)). In *Vizio*, the plaintiffs relied on conclusory allegations that communications were intercepted during their transmission and an "inscrutable graphic with no textual explanation" suggested that data was sent to defendant "significantly after the data arrive[d] at [plaintiffs'] Smart TVs." 238 F. Supp. 3d at 1228. Similarly, the *Rosenow* plaintiffs only alleged that defendants "knowingly and purposefully searched [p]laintiff's accounts," but did not allege *any* facts supporting an inference of data interception. *See* 2020 WL 1984062, at *7.

Here, Plaintiffs allege that Defendants intercepted biometric data by capturing still images of users' faces and facial recognition data (¶¶ 6, 39-44, 53-55) and then sent that data to Defendants' Amazon servers. ¶¶ 42-44. Defendants have acknowledged that these allegations are true. Indeed, Anker's "Customer Service Engineer specialized in safety and privacy" claimed it was ***necessary*** to intercept images being produced by the Camera Products "in real-time" to send notifications to consumers. *See* ¶ 55. Accordingly, because the intended recipient of the notification (the user) is receiving the product of an intercepted communication, the interception must, under Seventh Circuit precedent, be occurring contemporaneously with its transmission.

2. Anker Was Not a Party to Plaintiffs' Communications

While the Wiretap Act prohibits intentionally intercepting communications, parties to a communication or parties with prior consent are exempt from Section 2511(1)(a). 18 U.S.C. § 2511(2)(d). "The question here [turns on] . . . who the intended recipient of the communication was." *Kurowski v. Rush Sys. For Health*, 2023 WL 2349606, at *4 (N.D. Ill. March 2, 2023).

The Seventh Circuit has held that the duplicating and re-routing of communications constitutes a violation of the Wiretap Act. *See Szymuszkiewicz*, 622 F.3d at 706. In *Szymuszkiewicz*, the Seventh Circuit affirmed a Wiretap Act conviction, noting "the 'interception' of a

communication sent in packets must be done by programming a computer to copy the contents it sends. . . which was exactly what [defendant] told [victim's] computer to do." 622 F.3d at 706. To reach this conclusion, the Seventh Circuit necessarily held that a third-party which surreptitiously duplicates and reroutes an internet communication is not a "party" to a communication.

The outcome in *Szymuszkiewicz* contrasts with the Third Circuit's decision in *In re Google Inc.*, which concluded that any amount of fraud and deceit, including duplicating and rerouting, did not vitiate the party exception of 2511(2)(d). 806 F.3d 125, 143-44 (3d Cir. 2015). Other Circuit courts have rejected the Third Circuit's decision and agreed with *Szymuszkiewicz* as well. *See e.g.*, *In re Facebook Inc. Internet Tracking Litig.*, 956 F.3d 589, 607-08 (9th Cir. 2020); *see also In re Pharmatrak, Inc. Privacy Litig.*, 329 F.3d 9, 20-21 (1st Cir. 2003).

In the face of this precedent, Defendants still attempt to apply the *In re Google*'s reasoning within the Seventh Circuit. *See* Mot. at 8. But Plaintiffs here were led to believe that Anker's Camera Products recorded and stored videos and biometric data locally—features Defendants touted to differentiate the Camera Products from competitors' (¶¶ 2-4)—and communications through the eufy App were, therefore, expected to occur between Plaintiffs' own devices (*i.e.*, between Plaintiffs' Camera Products and Plaintiffs' phones). ¶ 10; *see Luis v. Zang*, 833 F.3d 619, 630-31 (6th Cir. 2016) (marketing materials supported inference that defendant violated Wiretap act).

Further, *Pharmatrak* supports finding that Anker was *not* a party to Plaintiffs' communications. There, the defendant argued that the court should infer that clients and their users had consented to defendant's interceptions. 329 F.3d at 19-21. But the court concluded that, where clients insisted that users' data not be collected and received assurances data would not be collected, "[defendant] ma[de] a frivolous argument" to suggest that clients and users somehow had notice of and impliedly consented to defendants' interception of plaintiffs' communications.

Id. at 21. Applying the defendant's theory that consent was obtained by "simply buying [defendant's] product" . . . "every online communication would provide consent to interception by a third party."

Plaintiffs' use of and reliance on the marketing for the Camera Products also is distinguishable from *Zak v. Bose Corp.*, where the plaintiff sued a smart device maker because the app captured music listening information while requesting media from music streaming services. 2019 WL 1437909, at *1-2 (N.D. Ill. March 31, 2019). While the plaintiff in *Zak* admitted the app was an intended part of the communication, he argued that the corporation was not. *Id.* at *3 n.5. The court did not dismiss plaintiff's theory of separating the app and corporation, but rather noted that plaintiff did not "point to any facts alleged to support such a distinction." *Id.*

Here, Plaintiffs allege facts that support the distinction between the app and the corporate entity. *E.g.*, ¶ 4 ("your recorded footage will be kept private. Stored locally. . . [a]nd transmitted to you, and only you"). Further, to the extent Defendants' position is that Anker's eufy App necessarily made Anker a party to communications, it would correspondingly render Anker's marketing that footage would be "transmitted to [the user], and only [the user]" false. *See* ¶ 4. Anker's response to the backlash after news broke of its data handling practices reinforces this point. If Anker had believed that the eufy App was a stand-in for the corporate entity, then Camera Products users would have and should have been put on notice of Anker's access to and collection of thumbnails through simple use of the App and Anker would not have needed to update its notification language. *See* ¶ 58 (Anker committed to "revising the push notifications language in the eufy App" to disclose cloud storage). Clearly, both users and Anker, at least as of January 2023, believed the App and corporate entity were distinct.

Plaintiffs thus sufficiently allege that Defendants intercepted Plaintiffs' communications (with or without the contemporaneous requirement), and because Anker was not a party to

Plaintiffs' communications, Plaintiffs have stated a Wiretap Act claim against Defendants.

B. Plaintiffs' BIPA Claims Are Adequately Plead

1. Plaintiffs Sufficiently Alleged That Defendants' Collected and Captured Biometric Information and Identifier

Defendants assert that Plaintiffs' claims that they "systematically collected, used, and stored" biometric data in violation of BIPA are "conclusory" and lack factual support. To the contrary, the Complaint more sufficiently alleges facts demonstrating that ***biometric identifiers*** or ***information*** are being ***collected***, ***captured***, or ***received***. 740 ILCS 14/15; *Stauffer v. Innovative Heights Fairview Heights, LLC*, 480 F. Supp. 3d 888, 907 (S.D. Ill. 2020) (To allege a violation of BIPA, "all [the plaintiff] must do is allege that Defendant collected, captured, purchased, received, or obtained her fingerprints without complying with BIPA's requirements."). "Biometric information" is defined as "***any information***, regardless of how it is captured, converted, stored, or shared, ***based on an individual's biometric identifier used to identify an individual***." 740 ILCS 14/10 (emphasis added). And "biometric identifiers" includes face geometry scans. *Id.* Thus, what matters is whether Plaintiffs alleged that Defendants collect ***any information based on an individual's face geometry scans*** that can be used to identify an individual.

Plaintiffs specifically allege that when the Camera Products recognize a face, they surreptitiously route the name, picture, and identification number associated with that face through Defendants' web servers before delivering the information to the user. ¶¶ 54-58. Plaintiffs further allege that Camera Products linked to separate accounts were able to identify a face with the same unique ID, meaning that Defendants were "not only storing facial recognition data in the cloud, but also sharing that back-end information between accounts." ¶ 6.[4] Defendants do not explain

[4] Indeed, Defendants' own press release, admits that at least one product did "send[ ] a user image from the eufy App to [Defendant's] devices [ ] to give the local facial recognition software a baseline to run its algorithm." Mot. Ex. B at 5. Accordingly, Defendants' assertion that Plaintiffs cannot support their

how this does not constitute the "collection" of "biometric information" under BIPA. This Court has already held that the collection of photographs can represent "biometric information" when they are used to identify individuals. *See Wilk v. Brainshark, Inc.*, 2022 WL 4482842, at *5 (N.D. Ill. Sept. 27, 2022). And despite Defendants' protestations otherwise, even general allegations suffice to survive a motion to dismiss. *See Johnson v. NCR Corp*., 2023 WL 1779774, at *2 (N.D. Ill. Feb. 6, 2023) ("Although NCR wants greater specificity at the pleading stage, Rule 9(b) does not apply to [ ] BIPA allegations"); *Wilk,* 2022 WL 4482842, at *5 (that defendant "obtained access to Plaintiff's uploaded video . . . used its technology to scan Plaintiff's facial geometry . . . and then developed reports" sufficiently alleged possession of biometric information).

Nevertheless, Defendants argue that Plaintiffs' allegations are "undermined" by the news articles on which the Complaint relies. Mot. at 12. This is disingenuous at best. Defendants cite an article from The Verge dated January 31, 2023, to suggest that Anker's cameras do not collect biometric information and that all "biometric details never leave users' devices." *Id.* citing Ex. B. Yet, the section of the article cited is a statement from Anker Innovations' Global Head of Communications. *See* Mot. Ex. B. at ECF pp. 5, 9-10. Put simply, Defendants cite their own self-serving press release to challenge the Complaint.[5] But there is good reason to take Defendants' press statement with a grain of salt. Defendants have admitted to making false statements and even the article stated that the company's press statements should not be trusted. *Id.,* Ex. B. at ECF pp. 2-3. If anything, the actual editorial portion of this article discredits Defendants' statement. Regardless, when evaluating a motion under Rule 12(b)(6), the Court may not weigh evidence, but

allegation that the BionicMind system purportedly performs facial recognition by "comparing the resulting 'face template' . . . against the face templates stored in a database" is contradicted by Defendants' statements. Mot. at 12-13.

[5] It is not entirely clear that such self-serving hearsay (within hearsay) would be admissible at trial. Accordingly, Defendants' press statements should not be taken as gospel here.

instead must accept the Complaint's allegations as true. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). Under the appliable standard, Plaintiffs' BIPA allegations are sufficiently pled.

2. BIPA Applies to the Putative National Class

Defendants' second argument against Plaintiffs' BIPA claims is more limited. Defendants do not contest that BIPA can be applied to the Illinois Plaintiffs and Class. Mot. at 14-15. Instead, Defendants argue that the national BIPA claims must be dismissed. *Id.* Defendants misunderstand the underlying law and allegations of the case.[6]

Defendants conveniently ignore the underlying basis for Plaintiffs' national BIPA class. Plaintiffs allege that Illinois law applies because Defendants agreed, through the Camera Products' End User License Agreement ("EULA"), that "any claim, dispute, action, cause of action, issue, or request for relief relating to this EULA, will be governed by the laws of Illinois, without giving effect to any conflicts of laws." ¶¶ 30, 120. Defendants do not claim that this agreement is invalid or inapplicable, nor could they. "When the parties express that intent (such as through a governing law provision), that express intent is generally recognized." *Smurfit Newsprint Corp. v. Se. Paper Mfg*., 368 F.3d 944, 949 (7th Cir. 2004).

Defendants ignore the choice-of-law provision in its own EULA, instead citing inapposite cases for the proposition that BIPA does not apply extraterritorially. Mot. at 14-15. For example, *Marsh v. CSL Plasma Inc*., 503 F. Supp. 3d 677 (N.D. Ill. 2020), and *Neals v. PAR Tech. Corp*., 419 F. Supp. 3d 1088 (N.D. Ill. 2019), are distinguishable because they did not involve a choice-

[6] As a threshold matter, the determination of the locus of Plaintiffs' BIPA claims for purposes of the extraterritoriality inquiry "is a highly fact-based analysis that is generally inappropriate for the motion to dismiss stage." *Vance v. Amazon.com, Inc.*, 525 F. Supp. 3d 1301, 1308 (W.D. Wash. 2021). "Accordingly, the majority of courts in BIPA cases to consider the issue at this stage have denied the motion to dismiss, opting instead to allow discovery for more information regarding the extent to which the alleged misconduct occurred in Illinois." *Id.* (collecting cases). Here, Defendants do not include any choice-of-law analysis, which one would normally associate with a request to strike national class allegations, instead relying on the generalized analysis from other cases. This is not enough to carry the day. *See Clay v. CytoSport, Inc*., 2018 WL 4283032, at *16 (S.D. Cal. Sept. 7, 2018).

of-law provision. Defendants' citation to *Avery v. State Farm Mutual Automobile Insurance Co*., 216 Ill. 2d 100 (2005), is also misplaced. *Avery* involved ICFA, which cannot be based on contract claims, and thus a contractual choice-of-law clause does not govern its application. *See Haught v. Motorola Mobility, Inc.*, 2012 WL 3643831, at *4 (N.D. Ill. Aug. 23, 2012).[7] Additionally, as *Avery* recognized, one of the elements of ICFA is that the deceptive trade practices occur "primarily and substantially within Illinois;" thus, even applying Illinois law, there must be some nexus between the defendant's actions and the state. *Id.*[8]; *Avery*, 216 Ill. 2d at 181-87.

These same considerations are not present in BIPA. Nothing in BIPA suggests that its private right of action is somehow incompatible with contractual claims. 740 ILCS 14/15(b). Instead, BIPA requires that parties execute some written agreement regarding the use of biometric identifiers or information. *Id*. Additionally, BIPA does ***not*** explicitly require collection of biometric information within the state or have any express geographical limits (unlike ICFA). *Compare* 740 ILCS 14/20 *with* 815 ILCS 505/1(f); *see Rivera v. Google Inc*., 238 F. Supp. 3d 1088, 1102 (N.D. Ill. 2017) ("in BIPA face scan context, even if the scanning takes place outside of Illinois, that would not necessarily be dispositive."). Instead, courts have "concluded that where a state law includes no express geographical limitation, courts may apply it to a contract that, because of a choice of law provision, falls under that state's law." *Harlow v. Sprint Nextel Corp*., 574 F. Supp. 2d 1224, 1226 (D. Kan. 2008); *Taylor v. E. Connection Operating, Inc*., 465 Mass. 191, 199 (2013). And this proposition has been cited with approval in Illinois state courts. *Int'l*

[7] Citing *Int'l Profit Assocs., Inc. v. Linus Alarm Corp.,* 2012 WL 2366404, at *7 (Ill. App. Ct. June 20, 2012) ("Particularly . . . where an action under the Act must be based *outside of contract,* it does not make sense to have a contractual choice-of-law provision automatically prevail over a statutory territorial limitation.").

[8] Citing *Shaw v. Hyatt Int'l Corp*., 2005 WL 3088438, at *3 (N.D. Ill. Nov. 15, 2005) (where choice-of-law provision on defendant's website specified Illinois law, the existence of such a clause has no impact on whether the ICFA applies in the first instance because the extraterritorial application of the ICFA is limited to deceptive trade practices occurring "primarily and substantially within Illinois).

Profit Assocs., Inc. v. Linus Alarm Corp., 2012 IL App (2d) 110958, ¶ 20 (2012) (citing *Gravquick A/S v. Trimble Navigation Int'l Ltd*., 323 F.3d 1219, 1223 (9th Cir. 2003)).

BIPA may be applied to this dispute through Defendants' choice-of-law provision. To hold otherwise would be fundamentally unfair, as it would allow the drafting party to demand that an agreement be governed by the law of a particular state, only to proclaim that the presumption against extraterritoriality precludes the application of the law when it is no longer favorable.

C. Plaintiffs State Claims for Violations of State Consumer Protection Statutes

1. Plaintiffs Have Pled Deceptive Conduct

All consumer protection statutes at issue—ICFA, FDUTPA, MCPL, and NY GBL—apply an objective standard to the question of whether a defendant's conduct or statements are materially misleading. Each asks, that is, whether the defendant's conduct or statements would deceive a reasonable consumer under the circumstances presented.[9] What is "reasonable" is generally a question of fact to be resolved by a jury.[10] Regardless, Defendants seek dismissal on the ground that Plaintiffs have failed to plead violations of the consumer protection statutes as a matter of law.

---

[9] *See, e.g., Carriuolo v. Gen. Motors Co.*, 823 F.3d 977, 984 (11th Cir. 2016) ("Under Florida law, an objective test is employed in determining whether the practice was likely to deceive a consumer acting reasonably."); *Campbell v. Drink Daily Greens, LLC*, 2018 WL 4259978, at *3 (E.D.N.Y. Sept. 4, 2018) (NY GBL §§ 349 and 350 ask "[w]hether a representation or an omission, the deceptive practice must be likely to mislead a reasonable consumer acting reasonably under the circumstances"); *Ash v. PSP Distrib., LLC*, 2023 WL 3939189, at *4 (Ill. App. June 12, 2023) ("Courts view the elements of a Consumer Fraud Act claim under an objective standard."); *Aspinall v. Philip Morris Cos., Inc.*, 813 N.E.2d 476, 486 (Mass. 2004) ("[A] practice is 'deceptive' . . . if it could reasonably be found to have caused a person to act differently from the way he [or she] otherwise would have acted.").

[10] *See, e.g., Kelly v. Beliv LLC*, 2022 WL 16836985, at *4 (S.D.N.Y. Nov. 9, 2022) (only in "'rare situation[s] [is] granting a motion to dismiss . . . appropriate' with respect to the issue of whether a reasonable consumer would be misled by representations about a product"); *Zurliene v. Dreyer's Grand Ice Cream, Inc.*, 591 F. Supp. 3d 362, 364 (S.D. Ill. 2022) ("[H]ow reasonable consumers would interpret an ambiguous . . . label is typically a question of fact that should not be decided on the pleadings.") (quoting *Bell v. Publix Super Markets, Inc.*, 982 F.3d 468, 478 (7th Cir. 2020)); *S. Broward Hosp. Dist. v. ELAP Servs.*, LLC, 2020 WL 7074645, at *4 (S.D. Fla. Dec. 3, 2020) ("[W]hether a practice is "deceptive or unfair" is determined by an objective analysis, and ordinarily is a question of fact for the jury to determine."); *Cremaldi v. Wells Fargo Home Mortg.*, 2015 WL 13849395, at *5 (D. Mass. Mar. 31, 2015) ("[W]hether a particular set of acts in their factual setting is unfair or deceptive is a question of fact[.]").

See Mot. at 15-23. Their efforts fail because (1) the privacy representations Defendants categorize as "puffery" are actionable misleading statements; (2) the remaining statements Plaintiffs challenge would deceive the reasonable consumer; (3) Defendants fail to address certain material misrepresentations alleged; and (4) Plaintiffs have pled materially misleading omissions.

2. The "Privacy" Statements Are Not Non-Actionable Puffery

Defendants contend that five statements challenged in the Complaint constitute non-actionable puffery. New York, Illinois, Massachusetts, and Florida law define "puffery" as "subjective claims . . . which cannot be proven either true or false" or "exaggerated, blustering, and boasting statements that are objective—and therefore technically provable—but upon which no reasonable buyer would [rely]." *Int'l Code Council, Inc. v. UpCodes Inc.*, 43 F.4th 46, 59 (2d Cir. 2022); *see Evolve Biosys., Inc. v. Abbott Lab'ys*, 2022 WL 846900, at *5 (N.D. Ill. Mar. 22, 2022) ("[C]ommercial statements are not puffery . . . if they make 'objective claims' that describe specific or absolute characteristics of a product capable of testing" or "if reasonable consumers could rely on them in their purchasing decisions"); *Thompson v. Procter & Gamble Co.*, 2018 WL 5113052, at *2 (S.D. Fla. Oct. 19, 2018) ("[U]nder FDUTPA, courts in this district have looked to whether the claims are specific and measurable, as opposed to vague and highly subjective."); *Martin v. Mead Johnson Nutrition Co.*, 2010 WL 3928707, at *3 (D. Mass. Sept. 30, 2010) ("Puffery" involves "outrageous generalized statements, not making any specific claims").

Critically, whether a statement constitutes "puffery" depends on context; statements challenged as such are not reviewed in a vacuum. *See, e.g., Avalanche IP, LLC v. FAM, LLC*, 2022 WL 3597411, at *6 (D. Mass. Aug. 23, 2022); *Evolve Biosys.*, 2022 WL 846900, at *5; *Thompson*, 2018 WL 5113052, at *2. The five representations Defendants cite are not "non-actionable puffery" (*see* Mot. at 18) because they go to the heart of the promotion of the Camera Products. Defendants sought to distinguish their products from their competitors' products on the ground

that the Camera Products prioritized data privacy. *See* ¶¶ 3, 31. Read in the context of the eufy marketing campaign, Defendants intended all five of these statements to induce consumers into believing that eufy products would provide superior protection for their data and videos. *See* ¶¶ 31, 38. This alone renders them actionable under the state consumer protection statutes at issue.[11]

Even were that not the case, at the very least, the last representation Defendants cite is, standing alone, a concrete statement "specific enough to induce consumer reliance." *Evolve Biosys.*, 2022 WL 846900, at *5. Plaintiffs' allegations directly contradict Defendants' assertion that they took "every step imaginable" to ensure that consumer data would remain "private, with you." Mot. at 18. Plaintiffs allege, *inter alia*, that data collected by eufy products was sent to Anker and to the Cloud and "was not protected using Military-Grade AES-256 data encryption," as represented, ¶¶ 41, 42, 44, 45; consumers were able to live-stream video footage from eufy camera products because the streams were not encrypted, *id.* ¶¶ 45; and facial-recognition data was uploaded and stored to Anker's servers, *id.* ¶¶ 39, 53, 55, 56. If Plaintiffs prove any of these allegations, they will have disproven Defendants' assertion that they took "every step imaginable" to ensure data privacy. This alone renders Defendants' statement actionable. *See, e.g.*, *Thompson*, 2018 WL 5113052, at *2 ("The Eleventh Circuit has found puffery where a representation was not the sort of empirically verifiable statement that could be affirmatively disproven."); *Evolve Biosys.*, *Inc.*, 2022 WL 846900, at *5 (commercial statements not puffery if they can be tested).

[11] *See, e.g.*, *Evolve Biosys.*, 2022 WL 846900, at *6 (statements that infant probiotic products were "stable," "potent," "high quality," and made from a "unique blend" not puffery because "commercial statements do not exist in a vacuum"); *In re Keurig Green Mountain Single-Serve Coffee Antitrust Litig.*, 383 F. Supp. 3d 187, 247 (S.D.N.Y. 2019) (qualifiers such as "perfect" not "puffery" in context in which they were used); *Marty v. Anheuser-Busch Cos., LLC*, 43 F. Supp. 3d 1333, 1342 (S.D. Fla. 2014) (representation that beer was of "German Quality" not puffery read in conjunction with other representations and overall marketing campaign); *Washtenaw Cnty. Emps.' Ret. Sys. v. Talbots, Inc.*, 2013 WL 5348569, at *30 (D. Mass. Sept. 23, 2013) (statements about "strong inventory management" not "inactionable puffery" where plaintiff was experiencing "widespread inventory management difficulties").

3. Defendants' Statements Regarding Storage and Streaming, Facial Recognition, and Encryption Could Deceive a Reasonable Consumer

Defendants also contend that certain misrepresentations about storage and streaming, facial recognition, and encryption are not misleading, arguing that Plaintiffs have only alleged facts that demonstrate that Defendants' representations are accurate. *See* Mot. at 19-21. Of course, "any challenge based on the actual truth or falsity of the statements is not appropriately raised on a motion to dismiss." *Keurig Coffee Antitrust Litig.*, 383 F. Supp. 3d at 247. Regardless, Defendants' argument is belied by a simple comparison of their representations to Plaintiffs' allegations:

Defendants' Representations	**Contradicting Allegations**
• "Storage[:] You are in control of your recordings. We have designed controls to ensure all videos are stored securely, in your home, on your local storage, with cloud storage available as an additional option." • "[N]o data [is] shared with third parties." ¶ 36. • "Whether it's your newborn crying for mom, or your victory dance after a game, your recorded footage will be kept private. Stored locally. With military-grade encryption. And transmitted to you, and only you." ¶ 11. • "On-Device AI[:] Our AI is built in to your security devices. It analyzes recorded video locally without the need to send it to the cloud for analysis." ¶ 33. • The camera products use "Military-Grade AES-256 data encryption." ¶¶ 11, 32. • "End-to-end Encryption[:] All recorded videos are encrypted from device to phone—only you have the key to decrypt and access your videos via the eufy Security app." ¶ 33	• Videos could be streamed and viewed using a third-party player, ¶¶ 7, 45, 47, 64, 65. • Thumbnails lifted from recorded videos were stored on Anker's AWS-hosted cloud storage. ¶¶ 42-44, 56, 57, 124. • Defendants conceded that thumbnails were sent to cloud server hosted by third party AWS. ¶¶ 56-58. • Camera Products did not use military-grade encryption. ¶¶ 42-45, 47, 54, 64-67. • Thumbnail images and name-tags were sent to cloud hosted by third party. ¶¶ 41-45, 47, 56-58. • "[D]ata associated with [consumers'] Camera Products was being sent to Anker and was not protected using Military-Grade AES-256 data encryption." ¶ 41, *see also id*. ¶¶ 42-45, 47, 54-58. • "[A] very weak AES key was being used to encrypt video footage, which could be easily brute forced." ¶¶ 42, 44. • "[T]he Camera Products were uploading name-tagged thumbnail images to Anker's AWS-hosted cloud storage, without encryption." ¶¶ 42-44, 56. • Recorded facial recognition information was uploaded to Anker's servers without being adequately secured. ¶ 53.

Defendants' contention that these representations could not mislead a reasonable consumer is further contradicted by the wealth of expert opinions that Defendants' marketing and advertising concealed the truth. Plaintiffs incorporate into the Complaint opinions by security experts and national publications that Defendants' representations about the Camera Products' encryption capabilities, local storage, and privacy protections were misleading at best. *See* ¶¶ 41-48. These opinions compel the conclusion that Plaintiffs have plausibly alleged that a reasonable consumer would also likely be misled. *See*, *e.g.*, *Zamber v. Am. Airlines, Inc.*, 282 F. Supp. 3d 1289, 1299 (S.D. Fla. 2017) ("If the statements are likely to mislead reasonable consumers, then it makes no difference if the statements are technically or literally true."); *People ex rel. Spitzer v. H & R Block, Inc.*, 16 Misc. 3d 1124(A), 847 N.Y.S.2d 903 (N.Y. Sup. Ct. 2007) (same).

Defendants' arguments to the contrary fail to persuade. Defendants contend that their "storage and streaming" representations could not plausibly mislead because these statements "are largely limited to recorded video footage," while Plaintiffs' allegations about storage and streaming describe the transmission of live footage, thumbnails, and personal identifying information to third-party sources. *See* Mot. at 19. Not so. The tenor of Defendants' security promises related to "data" generally. *See* ¶¶ 33, 36, 37. Even if "data" generally were not at issue, it is for a jury to decide whether Defendants' representations were "likely to mislead a reasonable consumer." *Campbell*, 2018 WL 4259978, at *3. It is also for a jury to decide whether a reasonable consumer would interpret thumbnails pulled from videos to constitute "recorded video footage." *See Bell*, 982 F.3d at 483; *Valcarcel v. Ahold U.S.A., Inc.*, 577 F. Supp. 3d 268, 280 (S.D.N.Y. 2021); *Zamber*, 282 F. Supp. 3d 1289, 1299 (S.D. Fla. 2017).

Defendants attack Plaintiffs' allegations about encryption on similar grounds, arguing that their statements about "end-to-end" encryption applied only to recorded video and that they never promised that "strong encryption was used for all data captured by the devices." Mot. at 20.

Defendants' contention is only possible by ignoring their representation that the Camera Products would protect consumers' data with "military-grade encryption." ¶¶ 4, 11, 13, 32, 42. Plaintiffs allege that Defendants did not use "military grade encryption" to protect data, live video streams or recorded video. *See id.* ¶¶ 7, 9, 10, 41-47, 54-58, 64-67. Regardless, neither the truth or falsity of Defendants' statements nor a reasonable consumers' interpretation of the terms used in the context presented is properly resolved on a motion to dismiss. *See* Section IV.B, *supra*; *see also* Section IV.C.2, *supra* (addressing Defendants' misrepresentations about facial recognition).

4. Defendants Fail to Address Six Misrepresentations Identified in the Complaint.

Defendants fail to address at least six misrepresentations found in their packaging or promotional materials. In addition to the misleading statements quoted in Defendants' motion (which Plaintiffs address below (Section IV.C.3, *supra*)), Defendants represented that consumers' data "is always safe" (¶ 33), "There is no online link available to any video"(*id.*), "[A]pp might collect only one type personal info—the user's email address" (¶ 36), "[D]ata never leaves the safety of your home, and is accessible by you alone" (¶ 33), "no one has access to your data but you" (¶ 37), and video footage is "sent straight to your phone—and only you have the key" (¶ 48).

Defendants cannot, on the pleadings, defend these representations as immaterial or nondeceptive. To be sure, Plaintiffs allege that Defendants violated every one of these promises. Plaintiffs allege, among other things, that Defendants collected consumer data from Plaintiffs and uploaded this information to Defendants' servers; security experts were able to access user video footage using an online link; the eufy App collected personal data, including thumbnail images and personally identifying information; and consumer data was uploaded to Defendants' cloud storage without encryption. *See id.* ¶¶ 42-67. These allegations alone warrant denial of Defendants' Motion. *See, e.g., Zurliene*, 591 F. Supp. 3d at 364 (how reasonable consumer would interpret

label is question of fact beyond pleadings); Section IV.C.1, *supra* (citing additional authority).

5. Plaintiffs Have Pled Material Misleading Omissions.

Finally, Defendants contend that Plaintiffs have not pled deceptive omissions because they have not plausibly alleged that (i) thumbnails and biometric information were stored on Defendants' cloud servers, (ii) such information was sent without encryption, or (iii) such information was "subject to facial recognition off of their devices." Mot. at 21. Plaintiffs dispose of Defendants' argument in Sections IV.A.1-IV.A.3 *supra*, *e.g.*, Defendants concede that Plaintiffs have alleged that thumbnails were sent to Anker's cloud server, which was hosted by a third party; and Plaintiffs have plausibly alleged that data and video streams were transmitted without encryption and were accessible to third parties, including facial recognition and other personally identifying information. *See* Sections IV.A.1, IV.B.1, *supra*.

6. Plaintiffs Have Plausibly Pled Causation

Defendants argue that Plaintiffs have not pled causation under their respective state consumer protection statutes with the particularity required by Rule 9(b). *See* Mot. at 21-23. Rule 9(b) does not apply to FDUTPA and NY GBL §§ 349 and 350 claims. *See Pelman ex rel. Pelman v. McDonald's Corp.*, 396 F.3d 508, 511 (2d Cir. 2005) (section 349); *Lewis v. Mercedes-Benz USA, LLC*, 530 F. Supp. 3d 1183, 1231 (S.D. Fla. 2021) (FDUTPA); *Am. Dev. Grp., LLC v. Island Robots of Fla.*, 2019 WL 5790265, at *10 (E.D.N.Y. Oct. 4, 2019) (section 350). In Massachusetts and Illinois, Rule 9(b) applies to consumer protection claims sounding in fraud. *See Timmins Software Corp. v. EMC Corp.*, 502 F. Supp. 3d 595, 605 (D. Mass. 2020); *Smith v. NVR, Inc.*, 2018 WL 6335051, at *2 (N.D. Ill. Dec. 5, 2018). Courts in Massachusetts and Illinois find that 9(b) is satisfied where "the complaint is sufficiently particular to inform the defendants of the nature of the claims against them, and those defendants are entirely capable of drafting an adequate response." *Petri v. Gatlin*, 997 F. Supp. 956, 975 (N.D. Ill. 1997); *see, e.g., Dumont v. Reily Foods*

Co., 934 F.3d 35, 39 (1st Cir. 2019) (description of label and subjective interpretation thereof sufficed: "This is not a case, after all, in which the defendant can claim that it never made the allegedly deceptive statement. Nor is this a case in which liability turns on more precise information concerning the 'when' or the 'where.' Rather, it turns on an assessment of the very particularly identified 'what' in the product label.").

In all four jurisdictions, "materiality and causation are established by a showing that the deceptive representation could reasonably be found to have caused a person to act differently from the way he [or she] otherwise would have acted." *In re M3 Power Razor Sys. Mktg. & Sales Prac. Litig.*, 270 F.R.D. 45, 60 (D. Mass. 2010).[12] None of the four consumer protection statutes requires a plaintiff to plead reliance. *Carriuolo*, 823 F.3d at 984 (addressing FDUTPA); *M3 Power Razor Sys*., 270 F.R.D. at 60 (MCPL); *Breeze v. Bayco Prod. Inc.*, 475 F. Supp. 3d 899, 905–06 (S.D. Ill. 2020); *Stutman v Chemical Bank*, 731 N.E. 2d 608, 612 (2000) (NY GBL § 349). Although reliance is generally required to state a section 350 claim for false advertising, "under New York law, there is a presumption of reliance when the defendant controls the relevant information and a consumer of ordinary intelligence could not discover the true state of affairs." *Guido v. L'Oreal, USA, Inc.*, 284 F.R.D. 468, 483 (C.D. Cal. 2012) (citing *Leider v. Ralfe*, 387 F. Supp. 2d 283, 293, 296 (S.D.N.Y. 2005)).

The Massachusetts, Florida, New York, and Illinois Plaintiffs have stated claims for violations of their states' consumer protection and false advertising statutes. All four Plaintiffs

[12] *See, e.g., Lewis*, 530 F. Supp. 3d at 1233 (plaintiffs pled FDUTPA causation by alleging that "[h]ad they been aware of the defect that existed . . . [they] either would have paid less for their vehicles or would not have purchased or leased the vehicle."); *Terrazzino v. Wal-Mart Stores, Inc.*, 335 F. Supp. 3d 1074, 1085 (N.D. Ill. 2018) ("[T]o properly plead the element of proximate causation in a private cause of action for deceptive advertising brought under the [ICFA], a plaintiff must allege that he was, in some manner, deceived."); *Rodriguez v. It's Just Lunch, Int'l*, 300 F.R.D. 125, 147 (S.D.N.Y. 2014) ("To satisfy the causation requirement [of section 349], nothing more is required than that a plaintiff suffer a loss because of defendants' deceptive act.")).

identify the products they bought and the date of purchase, and detail either the specific representations they reviewed or the category of representations together with the dates and locations thereof (*e.g.*, the privacy representations on the packaging or a specific website). *See* ¶¶ 11-14, 16,17. Though unnecessary, they also allege that they relied on the cited statements. *See id.* Finally, each Plaintiff alleges that he would not have purchased a eufy Camera Product, or would have paid less, had he known the truth about its actual capabilities. *See id.* These allegations suffice to satisfy Rule 8 and Rule 9(b). *See, e.g.*, *Dumont*, 934 F.3d at 39; *Crisostomo v. New Balance Athletics, Inc.*, 2022 WL 17904394, at *7 (D. Mass. Dec. 23, 2022) (plaintiff satisfied 9(b) by identifying date of purchase, statement on packaging, why it was misleading); *Terrazzino*, 335 F. Supp. 3d at 1085 (at pleading stage, allegations that deceptive conduct induced plaintiff to pay more than product's value and that plaintiff would not have bought the product but for the deceptive act suffice to plead causation in support of an ICFA claim); *Marty*, 43 F. Supp. 3d at 1346 (FDUTPA claims stated where plaintiff "alleges that he or she has paid a premium price for a product as a result of a defendant's misrepresentation"); *Guido*, 284 F.R.D. at 483 ("[W]here consumers allege that they paid a premium for the product based on marketing representations . .. they have adequately alleged an injury under § [349 or] 350.").

D. The Court Should Uphold Plaintiffs' Unjust Enrichment Claims

As Plaintiffs adequately plead violations of ICFA, NY GBL, MCPL, and FDUTPA, Defendants' sole argument for dismissal of the unjust enrichment claim fails. *See* Mot. at 24.

E. The Complaint Provides Defendants with Fair Notice of Plaintiffs' Claims

Defendants' Motion tacks on the assertion that the Complaint must be dismissed ***in its entirety*** because Plaintiffs refer to Defendants Anker Innovations, Fantasia, and Power Mobile collectively as "Anker" or "Defendants," which purportedly fails to provide Defendants with fair notice of Plaintiffs' claims ***as a matter of law***. Mot. at 24. Defendants are wrong.

As an initial matter, claims under the Wiretap Act, BIPA, NY GBL, FDUTPA, and unjust enrichment need only be pleaded to Rule 8's lenient notice standard.[13] Under Rule 8, "[t]here is no 'group pleading' doctrine, per se, that either permits or forbids allegations against defendants collectively; 'group pleading' does not violate Fed. R. Civ. P. 8 so long as the complaint provides sufficient detail to put the defendants on notice of the claims." *Robles v. City of Chicago,* 354 F. Supp. 3d 873, 875 (N.D. Ill. 2019). A complaint "provides sufficient notice to each defendant, despite employing a consistent 'group pleading' approach" where "allegations are directed at all the defendants." *Gorgas v. Amazon.com, Inc.*, 2023 WL 4209489, at *3 (N.D. Ill. June 23, 2023). In *Gorgas*, plaintiffs brought BIPA claims substantively identical to Plaintiffs', including that corporate affiliates—defined collectively as "Amazon"—captured and stored biometric data without consent and disclosed it to third parties. *Id.* The court held that the plaintiffs' references to "defendants" met the Rule 8 standard because "the allegations are directed at all the defendants." *Id.* Plaintiffs' Complaint, like the *Gorgas* complaint, alleges that ***all Defendants*** improperly captured class members' biometric data without permission and made the same misrepresentations about the Camera Products' privacy and security features to all members of the putative classes. *See* ¶¶ 27-67. The allegations underlying Plaintiffs' Wiretap Act, BIPA, NY GBL, FDUTPA, and unjust enrichment claims thus provide Defendants with sufficient notice of Plaintiffs' claims.

Although Plaintiffs' ICFA and MCPL claims may need to be pleaded with particularity, the Complaint's allegations are sufficient under Rule 9(b) because Plaintiffs cannot know, absent

[13] *See Wilk*, 2022 WL 4482842, at *5 (Rule 9(b) does not apply to [ ] BIPA allegations"); *Colpitts v. Blue Diamond Growers*, 527 F. Supp. 3d 562, 577 (S.D.N.Y. 2021) ("[c]laims under GBL §§ 349 [and] 350 . . . need only meet the bare-bones notice-pleading requirements of Rule 8(a)"); *Lewis*, 530 F. Supp. 3d at 1231 ("requirements of Rule 9(b) do not apply to claims under FDUTPA"); *Siegel v. Shell Oil Co.*, 480 F. Supp. 2d 1034, 1043–44 (N.D. Ill. 2007) (lower pleading standard applies to unjust enrichment because "claim [does not] require[] proof of an intentional misrepresentation"); *B & G Crane Serv., LLC v. Duvic*, 2006 WL 8434010, at *3 (M.D. La. Sept. 19, 2006) (acknowledging "the absence of a heightened pleading standard" for Wiretap Act), *report and recommendation adopted sub nom. B&G Crane Serv., LLC v. Duvic*, 2006 WL 8434230 (M.D. La. Oct. 17, 2006).

discovery, each Defendant's misconduct in misrepresenting their Camera Products and improperly collecting biometric data. *See e.g.*, *Wordlaw v. Enter. Leasing Co. of Chicago, LLC*, 2020 WL 7490414, at *3 (N.D. Ill. Dec. 21, 2020) (grouping pleading appropriate where plaintiff was "unable to allege which one in particular installed and controlled the timekeeping system"); *Cunningham v. Foresters Fin. Servs., Inc.*, 300 F. Supp. 3d 1004, 1016 (N.D. Ind. Jan. 9, 2018) ("Plaintiff cannot reasonably be expected to know" relationship between the corporate defendants "at this stage of litigation"). Here, as in *Wordlaw* and *Cunningham*, Plaintiffs allege specific misrepresentations about Defendants' products, why those misrepresentations were false and misleading, how Plaintiffs encountered those misrepresentations (*e.g.*, on labels and websites), and that Defendants are affiliates.[14] *See* ¶¶ 17-21, 31-37. Further, each Defendant is a private wholly owned subsidiary of a foreign corporation, and thus its internal processes are not publicly disclosed. *See id.* Accordingly, Defendants "are related corporations that can most likely sort out their involvement without significant difficulty," *Jepson, Inc. v. Makita Corp.*, 34 F.3d 1321, 1329 (7th Cir. 1994), and any purportedly omitted allegations can be easily identified in discovery.

Defendants' cases do not hold otherwise. As an initial matter, *none* of the cases cited in the Motion hold that group pleading is insufficient under Rule 8 as a matter of law, and thus Defendants do not provide ***any*** authority supporting dismissal of Plaintiffs' Wiretap Act, NY GBL, BIPA, FDUTPA or unjust enrichment claims. *See* Mot. at 24-25 (citing cases).

Nor do Defendants' cases support dismissing Plaintiffs' ICFA or MCPL claims. In *SEC v. Winemaster*, 529 F. Supp. 3d 880, 907 (N.D. Ill. 2021), and *Jepson,* 34 F.3d at 1329, the courts held that the plaintiffs' allegations ***were*** sufficient under Rule 8—and the *Jepson* plaintiffs referred

[14] Anker Innovations and Fantasia's Rule 7.1 disclosure in this action confirmed that they are affiliates, as did Power Mobile's Rule 7.1 disclosure in another recent case. *See* ECF No. 15 at 1; Corp. Discl. Stmt., *Brady v. Anker*, No. 7:18-cv-11396 (S.D.N.Y. Jan. 18, 2019), ECF No. 17. Defendants also acknowledge that they are "alleged to be members of a corporate family." Mot. at 25.

to defendants collectively. *See id.* Defendants' remaining cases involved plaintiffs who should have been able to plead specific misconduct because, unlike Plaintiffs, they had direct contact with specific defendants. *See Cornielsen v. Infinium Cap. Mgmt., LLC*, 916 F.3d 589, 600–01 (7th Cir. 2019) ("[p]laintiffs have no recollection of who said what, even though each [p]laintiff personally observed which representations [each defendant] made on particular days"); *Rocha v. Rudd*, 826 F.3d 905, 912-13 (7th Cir. 2016) (second amended complaint identified communications from specific defendants)[15]; *SEC v. Kameli*, 373 F. Supp. 3d 1194, 1204 (N.D. Ill. 2019) ("the SEC has at least as much access to the investors as defendants and so has, or can gather, the needed details").

F. Plaintiffs Respectfully Request the Opportunity to Amend

Should the Court dismiss any portion of the Complaint, Plaintiffs respectfully request leave to replead pursuant to Fed. R. Civ. P. 15, under which leave to amend should be "freely given when justice so requires" absent delay, bad faith, dilatory motive, futility, prejudice or repeated failure to cure deficiencies. *See Ferguson v. Roberts*, 11 F.3d 696, 706 (7th Cir. 1993).

V. CONCLUSION

As set forth above, the Court should deny Defendants' Motion in its entirety.

Dated: July 7, 2023

Respectfully submitted,

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC

/s/ *Gary M. Klinger*

Gary M. Klinger
227 W. Monroe Street, Suite 2100
Chicago, Illinois 60606
Telephone: 866.252.0878
gklinger@milberg.com

[15] *See* Compl., *Rocha v. Rudd*, No. 14-cv-04857 (N.D. Ill. Nov. 20, 2014), ECF No. 37-1 (¶¶ 31, 37, 141, 144).

POMERANTZ LLP
Jeremy A. Lieberman
Brian Calandra
600 Third Avenue, 20th Floor
New York, New York 10016
Telephone: (212) 661-1100
Facsimile: (212) 661-8665
jalieberman@pomlaw.com
bcalandra@pomlaw.com

Attorneys for Lead Plaintiffs and the Putative Classes

LEVI & KORSINSKY, LLP
Mark S. Reich*
Courtney E. Maccarone*
Gary I. Ishimoto*
55 Broadway, 10th Floor
New York, NY 10006
Telephone: 212-363-7500
Facsimile: 212-363-7171
Email: mreich@zlk.com
Email: cmaccarone@zlk.com
Email: gishimoto@zlk.com

KOZYAK TROPIN & THROCKMORTON LLP
Benjamin Widlanski, Esq.
Florida Bar No. 1010644
bwidlanski@kttlaw.com
Robert J. Neary, Esq.
Florida Bar No. 81712
rn@kttlaw.com
2525 Ponce de Leon Blvd., 9th Floor
Coral Gables, FL 33134
Tel: (305) 372-1800
Fax: (305) 372-3508

RENNERT VOGEL MANDLER & RODRIGUEZ, P.A.
Robert M. Stein, Esq.
Florida Bar No. 93936
rstein@rvmrlaw.com
Daniel S. Maland, Esq.
Florida Bar No. 114932
dmaland@rvmrlaw.com
100 SE 2nd Street, 29th Floor

Miami, FL 33131
Tel: (305) 423-3437
Fax: (305) 376-6176

TOUSLEY BRAIN STEPHENS PLLC
Kim D. Stephens, WSBA #11984
Jason T. Dennett, WSBA #30686
Rebecca L. Solomon, WSBA #51520
1200 Fifth Avenue, Suite 1700
Seattle, WA 98101
Telephone: (206) 682-5600
Facsimile: (206) 682-2992
Email: kstephens@tousley.com
Email: jdennett@tousley.com
Email: rsolomon@tousley.com

Additional Counsel for Plaintiffs and the Putative Class

CERTIFICATE OF SERVICE

I hereby certify that on this 7th day of July, 2023, I caused a true and correct copy of the foregoing notice to be filed with the Clerk of the Court for the Northern District of Illinois via the Court's CM/ECF system, which will send notification of such filing to the counsel of record in the above-captioned matters.

/s/ Gary M. Klinger
Gary M. Klinger